REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
04-05-2012	Final	

4. TITLE AND SUBTITLE
Joint Command and Control of Cyber Operations:
The Joint Force Cyber Component Command (JFCCC)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Maj Jason P. Quinter USMC

Paper Advisor (if Any): Prof Mike Croskrey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT: The evolution of technology has introduced sophisticated means to store, process, and transport information. Because the U.S. military establishment relies so heavily on complex command and control systems and interconnectivity in general, cyber warfare has become a serious topic of interest at the operational level of war. Joint doctrine acknowledges the impact of information technology advancements on the tempo, lethality, and complexity of warfare. Combatant Commands routinely confront unique challenges related to cyber space as they attempt to conceptualize and integrate offensive and defensive cyber warfare into current and future operations and plans. In particular, Joint Task Force (JTF) Commanders must develop an optimum method to command and control cyber forces. Comparing and contrasting the warfighting domains and historical introduction of nascent technologies will help to develop a command and control structure that effectively supports cyber operations. This paper recommends establishing a functional cyber component command within the joint task force as the optimal way to command and control cyber operations.

15. SUBJECT TERMS
Cyber war, cyber operations, command and control, command relationships

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION**	**18. NUMBER**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Joint Command and Control of Cyber Operations: The Joint Force Cyber Component Command (JFCCC)

by

Maj Jason P. Quinter USMC

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

4 May 2012

Contents

Abstract

The evolution of technology has introduced sophisticated means to store, process, and transport information. Because the U.S. military establishment relies so heavily on complex command and control systems and interconnectivity in general, cyber warfare has become a serious topic of interest at the operational level of war. Joint doctrine acknowledges the impact of information technology advancements on the tempo, lethality, and complexity of warfare. Combatant Commands routinely confront unique challenges related to cyber space as they attempt to conceptualize and integrate offensive and defensive cyber warfare into current and future operations and plans. In particular, Joint Task Force (JTF) Commanders must develop an optimum method to command and control cyber forces. Comparing and contrasting the warfighting domains and historical introduction of nascent technologies will help to develop a command and control structure that effectively supports cyber operations. This paper recommends establishing a functional cyber component command within the joint task force as the optimal way to command and control cyber operations.

Introduction

The evolution of technology has introduced sophisticated means to store, process, and transport information. Because the U.S. military establishment relies so heavily on complex command and control systems and interconnectivity in general, cyber warfare has become a serious topic of interest at the operational level of war. Joint doctrine acknowledges the impact of information technology advancements on the tempo, lethality, and complexity of warfare.[1] Combatant Commands routinely confront unique challenges related to cyber space as they attempt to conceptualize and integrate offensive and defensive cyber warfare into current and future operations and plans. In particular, Joint Task Force (JTF) Commanders must develop an optimum method to command and control cyber forces. Comparing and contrasting the warfighting domains and historical introduction of nascent technologies suggests a command and control structure that effectively supports cyber operations.[2] Establishing a functional cyber component command within the joint task force is the optimal way to command and control cyber operations.

Background

National security professionals are working to develop a comprehensive understanding of the nature of cyberspace in order to make critical decisions about how to fight effectively within and through it. This is a daunting task because many inherent characteristics of cyberspace make it difficult to comprehend. For instance, the pliable aspects of the cyber environment make cyber operations hard to conceptualize. Equally challenging to understanding cyberspace, yet having dramatic impacts, is the subtle nature of the environment. For example, determining whether an

[1] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 02 May 2007 Incorporating change 1, 20 March 2009), I-7 (CH 1).
[2] The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces http://www.brookings.edu/papers/2011/0715_cyber_forces_hathaway.aspx (accessed April 18, 2012).

act in cyberspace is of a hostile nature is difficult. Some cyber warfare theorists struggle to differentiate between those hostile acts that might lead to war and those that are cybercrime. This is significant because cyber warfare and cybercrime cross boundaries in U.S. law between Title 50 (War and National Defense), Title 10 (Armed Forces), Title 18 (Crimes and Criminal Procedures), and Title 6 (Domestic Security) of the U.S. Code.

Attribution is also a challenge in cyber warfare. Following a cyber-attack, a network address can be traced through efforts known as cyber forensics. Nevertheless, it is almost impossible to "identify with proof" who originated the attack because hackers have become proficient at working through proxies.[3] To further complicate matters, a cyber-attack by a non-state actor must be prosecuted differently than if proof existed that the attack was initiated by a hostile state military.

Despite the many unique aspects of the cyber environment, the intrinsic nature of warfare in cyberspace does not differ from warfare in other contexts. Warfare in cyberspace can still be considered a clash of hostile, independent, and irreconcilable wills each trying to impose itself on the other.[4] Friction is just as prevalent in the cyber environment as it is in any other environment. Cyber-attacks rarely achieve enduring effects. A network can be poorly defended, and intrusions can go undetected for undefined periods of time. Still, once the defender detects a malfunction in a system or loss of information on a network, code can be patched rather quickly. Regardless of whether intellectual property is lost or physical damage is done to a network, cyber-attacks will cause friction just like offensive operations do in any other environment.

[3] In this case, a proxy could be a single internet protocol (IP) address from a different network or sub network that may or may not even be located in close physical proximity to the attacker.
[4] U.S. Marine Corps, *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1 (Washington, DC: HQ U.S. Marine Corps, 1986), 3.

Uncertainty also prevails in the cyber environment. Even the finest intrusion detection systems and most effective cyber defensive measures will not fully prevent determined attacks. It is even more difficult to predict when and how attacks will take place in cyberspace than it is in other environments. On the sea or land, warfighters can rely on actionable intelligence preparation of the operating environment. However, in cyberspace it is virtually impossible to predict an attack in a similar fashion.

The complexity inherent to the cyber environment should also be considered. In fact, complexity is what makes it so difficult to comprehend fully the entire spectrum of cyber operations. Information technology becomes more difficult to understand as it evolves. Cyber operations have become so elaborate that many aspects affect other operational functions. For that reason, JTF Commanders must conduct persistent, critical analysis to determine the best way to command and control cyber operations.

In addition to friction, uncertainty, and complexity, many other aspects of the cyber environment are common to warfare in general. Fundamentally important, however, is that the nature of warfare is similar regardless of the environment. Although aspects of cyberspace are unique, the justification for establishing a command and control structure to manage cyber operations within the JTF is not solely because cyberspace is so different from other environments. To be clear, the argument is centered on developing the most effective way to command and control a new type of warfare when the geographic combatant command (GCC) activates a JTF. This is not to say that some of the complicated characteristics of cyberspace could not by themselves merit experimenting with a new command and control structure, because they could. Of the many different ways a JTF Commander can command and control

full spectrum cyber operations, analysis suggests that one method in particular may be the most effective.

There are various opinions concerning what to call the cyber battle space because it is so ubiquitous and omnipresent. Is cyberspace an environment, a medium of conflict, or a domain?[5] For years, the Department of Defense (DOD) has recognized air, land, sea, and space as individual domains. Most recently, joint doctrine has declared cyberspace to be a global domain.[6] According to Richard Crowell, cyberspace defines a fifth domain wherein warfighters must learn to operate and fight.[7] If operations are conducted in the air and space and on the land and sea, operations are conducted in and through the cyber environment. Project Air Force, a private report by the RAND Corporation, states:

> Cyberspace is a thing of contrasts: It is a space and is thus similar to such other media of contention as the land and sea. It is also a space unlike any other, making it dissimilar. Cyberspace has to be appreciated on its own merits; it is a man-made construct.[8]

The fact that cyberspace is manmade means that it is pliable. Consequently, the physical aspect of the domain can be altered in different ways. Ultimately, strong arguments can be made for referring to cyberspace as an environment, a medium of conflict, or a domain. Notwithstanding, these arguments are mostly semantic. The U.S. joint warfighting community must address the optimal way to leverage cyberspace and not become overly obsessed with what to call it.

---

[5] According to JP 1, joint publications now use the term "operational environment" where the term "battlespace" was used previously. The term "battlespace" is being replaced by the term "operational environment" in joint doctrine as joint publications are revised.

[6] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 8 November 2010 as amended through 15 February 2012), 83.

[7] Richard M. Crowell, " War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare V1.5," 3.

[8] Martin C. Libicki, "Cyberdeterrence and cyberwar," Rand Corporation: Project Air Force, 11.

Thorough examination of the nature and characteristics of the cyber environment naturally leads to an analysis of the best way to command and control forces in cyberspace.

> To date, our time and resources have focused more on network defenses to include firewalls, anti-virus protection, and vulnerability scanning. While generally effective against unsophisticated hackers, these measures are marginally effective against sophisticated adversaries. History teaches us that a purely defensive posture poses significant risks; the "Maginot Line" model of terminal defense will ultimately fail without a more aggressive offshore strategy, one that more effectively layers and integrates our cyber capabilities. If we apply the principles of warfare to the cyber domain, as we do the sea, air, and land, we realize the defense of the nation is better served by capabilities enabling us to take the fight to our adversaries, when necessary to deter actions detrimental to our interests.[9]
>
> *General James Cartwright, Vice Chairman, U.S. Joint Chiefs of Staff, 2007*

The current command and control structure for joint cyber operations must be evaluated and discussed prior to proposing a new arrangement. In cyberspace, DOD has primarily immersed in computer network defense because the Armed Services were not authorized to conduct computer network attack (CNA). For years, offensive CNA has been the exclusive province of the National Security Agency (NSA). Although CNA has been included in joint doctrine as a function of Information Operations, the military has invested minimal resources in developing a balanced concept for operating in and through cyberspace, choosing instead to focus purely on defensive fundamentals.

The current edition of Joint Publication 3-13, *Information Operations,* sufficiently addressed command and control of computer network operations when initially published. However, this publication is no longer sufficient to the modern cyber environment because it was

[9] James E. Cartwright, Statement on the United States Strategic Command Before the House Armed Services Committee, March 21, 2007. At the time of this statement, General Cartwright commanded the U.S. Strategic Command.

published before cyber became such an all-inclusive, integral part of operations.[10] Currently, joint forces at the operational level of war tend to leverage cyberspace similarly to the way it is leveraged at the national-strategic level. Specifically, there is an obsession with computer network defense and intrusion detection, and insufficient attention on how to truly operationalize cyberspace both offensively and defensively.

Command authority over joint cyber forces has been divided among U.S. Strategic Command (USSTRATCOM), the GCCs, and the military Services. The National Military Strategy for Cyberspace Operations, the Unified Command Plan, DOD Directive O-8530.1, and the Standing Rules of Engagement all apply to command and control of cyberspace operations. Unfortunately, guidance published in these documents is sometimes contradictory, and responsibilities often overlap. It is, therefore, essential for GCCs to decide how to organize and execute cyber operations effectively, especially when a crisis requires that a JTF be activated. Although the aforementioned strategies and additional supporting documentation hints at the proposition of a more centralized command and control structure for the conduct of cyber operations, this would be a largely ineffective way to organize the force. Inherent to U.S. joint doctrine are the tenets of centralized command and decentralized control. Therefore, the command and control structure for cyber operations must be consistent with existing joint force structure.

During the last two years, several cyber strategies have been developed and published at the strategic level. The National Strategy to Secure Cyberspace, the Comprehensive National Cybersecurity Initiative (CNCI), and the DOD Strategy for Operating in Cyberspace have all

[10] U.S. Government Accountability Office Report to Congressional Requesters, *Defense Department Cyber Efforts – DOD Faces Challenges In Its Cyber Activities*, GAO 11-75 (Washington, DC: GAO, July 2011) 10.

promulgated overarching strategic guidance for the conduct of cyber operations. Similar documents have been published by the individual military Services, but specific operational level guidance is still forthcoming. Regardless of how long it may take to develop an effective joint operational concept for cyber operations, the U.S. military will move forward intent on executing full spectrum operations in cyberspace.

Similar to the strategic emphasis on cyberspace doctrine and policies, cyber force structure has also been focused mainly at the strategic level. Until the last two years, DOD managed computer network operations through multiple organizations. In order to operationalize its missions, USSTRATCOM, tasked with operating and maintaining the global information grid (GIG), delegated operational and tactical level planning, force execution, and day-to-day management of forces to its joint functional component commands. First, the Joint Functional Component Command for Network Warfare (JFCC-NW) planned, integrated, and coordinated cyberspace capabilities and integrated all necessary computer network operations capabilities. Next, the Joint Task Force–Global Network Operations (JTF-GNO) operated the DOD's global network and directed the operation and defense of DOD's GIG. Finally, the Joint Information Operations Warfare Center was the lead entity responsible for planning, integrating, synchronizing, and advocating for information operations across DOD including computer network operations and electronic warfare.[11]

In 2009, U.S Cyber Command (USCYBERCOM) was formed as a sub-unified combatant command within USSTRATCOM. Consequently, JFCC-NW and JTF-GNO were disestablished to prevent a duplication of effort, a waste of resources, and a parallel command and control structure. Furthermore, DOD directed the military departments to provide appropriate component support to U.S. Cyber Command by assigning, allocating, and apportioning qualified personnel

[11] Ibid, 21.

for joint cyber operations. However, even though DOD has assigned authorities and responsibilities for implementing cyber operations among the GCCs and military Services, the supporting relationships necessary to achieve effective command and control of cyber operations remain unclear.[12]

Discussion

According to the *National Military Strategy for Cyberspace Operations,* the United States can achieve superiority in cyberspace only if command and control relationships are clearly defined and executed.[13] Unified Combatant Commanders have the authority to designate objectives, and to organize and employ forces in order to accomplish the command's mission. Combatant Command (COCOM) is normally exercised through subordinate Service or functional component commanders.[14] A Combatant Commander (CCDR) will often grant subordinate JTF Commanders operational control (OPCON). Therefore, all options must be explored to determine the best way to command and control cyber operations within a JTF.

One effective way for a JTF to command and control cyber operations would be to establish a Joint Force Cyber Component Commander (JFCCC) along functional lines. As mentioned, cyber operations are becoming a main focus of effort at the operational level of war. The command and control structure within a JTF is centered on the mission, concept of operations (CONOPS), objectives, and capabilities of subordinate forces.[15] Therefore, with future objectives and CONOPS being more focused on cyber warfare it would be logical to command and control these operations along functional lines. This line of reasoning also justifies

[12] U.S. Government Accountability Office Report to Congressional Requesters, *Defense Department Cyber Efforts – DOD Faces Challenges In Its Cyber Activities,* GAO 11-75 (Washington, DC: GAO, July 2011) 10.
[13] Department of Defense, *Fiscal Year 2011-2015 Capability Gap Assessment Results and Recommendations for Mitigating Capability Gaps,* JROCM 113-09 (Washington D.C., June 2009).
[14] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 02 May 2007 Incorporating change 1, 20 March 2009), IV-3 (CH 1).
[15] Ibid, IV-15.

a reduction of the JTF Commander's span of control because cyber operations significantly complicate the joint operating area (JOA), and increase size and capabilities of friendly forces.

Another way to command and control cyber operations within a JTF is to isolate responsibility for computer network operations (CNO) within the information operations (IO) cell of the JTF Operations Directorate (J-3). This option would be in favor of maintaining the status quo because current joint IO doctrine describes CNO as a function of IO. According to JP 3-13, "IO coordinates and synchronizes the employment of the five core capabilities in support of the combatant commander's objectives or to prevent the adversary from achieving his desired objectives."[16] One of those core capabilities is CNO. However, most key aspects of cyber-attack and defense are set apart from IO and are more aligned with the operational functions of intelligence and command and control.

The JTF Commander could also command and control all cyber operations within the JTF Communication Systems Directorate (J-6) and thus totally disassociate CNO from JTF J-3. This option suggests a more technical solution to the problem, and more centralized command and control. Much like IO is already doctrinally established within the J-3, computer network defense (CND) and information assurance (IA) are sub-functions of the J-6. This is mainly because CND and IA are regulated on the GIG by the Defense Information Systems Agency (DISA), which works in close coordination with USCYBERCOM and the DOD Command, Control, Computers, Communication (C4) community writ large.

Finally, a Unified GCC could retain OPCON of all joint cyber forces even after activating a JTF. This option would be most appropriate if more than one JTF were operating simultaneously in the same theater. The GCC would control joint cyber forces to support the

[16] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 13 February 2006), II-1.

objectives of multiple JTF Commanders while balancing theater wide GCC cyber priorities. Although maintaining OPCON of an entire "line of operation" is fairly uncommon, it is an option nonetheless. Of the options discussed in this paper, this alternative would enable the most centralized command and control structure.

Conclusions

There are multiple reasons why designating a JFCCC is the best option for full spectrum cyber warfare. One of the many advantages to establishing a more focused command and control structure for cyber operations is improved unity of effort. Establishing a JFCCC would also maintain unity of command through well-defined command relationships, an unambiguous chain of command, and clear delineation of responsibilities in accordance with requirements set forth in JP 1.[17] Currently, offensive and defensive computer network operations (CNO) are a subcomponent of information operations. Organic computer networks within the JTF are established, maintained, and defended by and for individual Service components. While this does not necessarily inhibit internal or external JTF communication, it is not the most effective way to employ or manage these network resources. Integrating like capabilities from each military Service into a single JFCCC support structure would be simple and efficient. Furthermore, this arrangement would support the entire JTF and facilitate synchronized offensive and defensive cyber operations.

There is one disadvantage associated with integrating the capabilities of each Service under the JFCCC. Similar to other functional components within the JTF, Service-organic JFCCC forces would have to achieve interoperability. This would be difficult because assigned or attached forces from each military Service would provide and employ dissimilar C4 personnel

[17] Chairman, U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, 02 May 2007 Incorporating change 1, 20 March 2009), IV-19 (CH 1).

and equipment to the JFCCC. In order to integrate people and equipment successfully from across the military Services, the DOD must synchronize how the Services man, equip, and train their cyber forces.

People who view CNA as a type of non-kinetic fires are proponents of keeping the cyber core capability within the fires cell of the JTF Operations Directorate (J-3). One advantage of this option is the likelihood that joint fires would be effectively synchronized because the span of control for offensive cyber operations would not be reduced. Some people would also argue that it is an attractively simple option, and it is. However, a disadvantage to this argument is that it only addresses offensive cyber warfare and fails to acknowledge the computer network defense aspect of CNO. The offensive and defensive aspects of cyber warfare are intrinsically linked and must not be separated. Continuing to treat cyber as a subcomponent of IO is short-sighted and outdated. Cyber operations must be conceptualized differently in order to develop new command and control schemes that best support full spectrum joint cyber warfare at the operational level.

Another disadvantage to this alternative is that it would not achieve unity of command or unity of effort for full spectrum cyber operations. While offensive cyber operations may be unified, they would not be synchronized with defensive operations. Cyber operations have become far too complex to be managed as a subcomponent of IO or anything else. It can be argued that IO requires CNO support, but that CNO should no longer be a core capability of IO. Cyber operations have evolved to such an extent that joint IO doctrine must be revised.

There are also advantages and disadvantages to disassociating CNO from the J-3 and using the J-6 to command and control all joint cyber operations. Communicators operating under the direction and supervision of the J-6 are adept at installing and maintaining complex computer networks. However, it would be unrealistic to expect the J-6 to accomplish these two mission

essential tasks concurrently with full spectrum offensive and defensive cyber operations. Furthermore, conducting all CNO within the J-6 would increase the JTF Commander's span of control, make it difficult to achieve unity of effort, and add to the complexity of the command and control structure. Even though personnel with CNO military occupational specialties are most qualified to execute full spectrum cyber operations, a failure to manage cyberspace in a holistic manner as is done with other domains severely underestimates the scope of cyber warfare.

Like the options previously mentioned, there are also advantages and disadvantages to maintaining OPCON of cyber forces at the GCC. One advantage is that the GCC has more resources available for employment and the flexibility to provide them quickly to the JTF when necessary. The GCC as the supporting commander would determine the tactics, forces, methods, procedures, and communications to be used in providing cyber support. Conversely, there are multiple disadvantages to this option. First, this command and control relationship is abnormal and complicated since the GCC would be supporting the subordinate JTFs instead of the other way around. Next, this alternative would rely on a more centralized command and control structure. As previously mentioned, this would be a significant divergence with established joint doctrine. Finally, maintaining OPCON of cyber forces at the GCC would fail to reduce the span of control. The GCC would be required to focus a great deal of effort on supporting cyber operations, which would detract from other functional areas.

There are multiple ways to command and control JTF cyber operations effectively. Each option has associated pros and cons, yet one alternative stands out as the best choice. Maintaining command and control of cyber forces within the JTF J-3 or J-6 increases the span of control of the JTF Commander, does not achieve unity of effort or command, and is far too

centralized. In contrast, designating a JFCCC reduces the span of control, increases unity of effort and command, helps synchronize offensive and defensive cyber operations, and is the simplest option available to the JTF Commander.

Recommendations

Thorough examination of alternatives suggests that the JFCCC is the optimum joint command and control structure for full spectrum cyber operations. If a JFCCC is established within a JTF, the JTF Commander must determine who will lead this component and what command authority they will be granted. The historical precedent is for functional component commanders (FCC) to serve concurrently as Service component commanders. The military Service that allocates or apportions the preponderance of the forces to the JTF often sources the FCC. It would be prudent to handle the JFCCC in the same fashion. As a FCC, the JFCCC should exercise OPCON of parent Service forces and tactical control (TACON) of cyber forces from other Services in accordance with doctrine outlined in JP 3-33.[18]

The JTF Commander must identify the JFCCC's specific responsibilities for the execution of FCC duties. All operational activities, including cyber, are designed to support accomplishment of the JTF mission and objectives. Therefore, cross-coordination between the JFCCC and other JTF components will be essential in order to integrate cyber operations fully into applicable plans and orders. The JFCCC should also provide mutual support to the other FCCs by conducting offensive CNO against designated targets in the joint operations area (JOA). For that reason, liaison officers (LNO) between the JFCCC and supported FCCs would be necessary.

[18] Chairman, U.S. Joint Chiefs of Staff, *Joint Task Force Headquarters*, Joint Publication (JP) 3-33 (Washington, DC: CJCS, 16 February 2007), III-2.

The JTF Commander should also consider requiring the JFCCC to serve as his principal advisor on the proper employment of all cyber forces. As the FCC for cyber operations, the JFCCC would centrally direct, allocate, and task available cyber forces and make cyber apportionment recommendations to the JTF Commander when appropriate. Under most circumstances, the JFCCC would be a supporting commander. Accordingly, cyber forces would be attached to other component commanders in support of their operations.

The JFCCC will require a joint component staff with appropriate representation from any Service that assigns or attaches cyber forces to it. Due to the complex nature of cyber operations, it would be prudent for USCYBERCOM to establish at least two deployable joint task force cyber augmentation cells (DJCAC) modeled after the global standing joint force headquarters (GSJFHQ). Upon the establishment of a JTF, one of these DJCACs would be attached to the JFCCC to serve as the core of its command element. Ultimately, the close working relationships within the DJCAC would facilitate unity of effort and unity of command within the JFCCC, and improve integration and synchronization of the entire staff.

The JFCCC staff would be designed with primary staff, special staff, and joint force staff directorates. Each staff directorate would accomplish its normal functions (primary or special) and some directorates would make unique contributions, as well. Some would even be combined for efficiency. Most prominent would be the combination of the operations (J-3), communication systems (J-6), and intelligence directorates (J-2) into a single cyber directorate (J-C). As a possible construct, commanders assigned as a JFCCC should consider dividing the J-C into the following three cells: a cyber-defense cell (J-CD), a cyber-attack cell (J-CA), and a cyber-exploitation cell (J-CE). These 3 cells would take the place of the traditional J-6, J-3, and J-2

directorates respectively. Forming this non-doctrinal J-C directorate would fuse all available cyber capabilities and synchronize full spectrum cyber operations. (see Appendix A)

Within the J-CE cell there would be LNOs from NSA, CIA, and the Defense Intelligence Agency (DIA). These representatives would serve as connecting files between operational and national strategic cyber forces. Additionally, they would ensure the availability of reliable signals intelligence, and provide timely indications and warnings of key characteristics in the cyber environment. Unlike the JTF Intelligence Directorate, the J-CE cell within the J-C directorate would focus exclusively on the cyber environment, working closely with the J-CD and J-CA cells. Ultimately, mission success would depend heavily on the J-CE's ability to collect and disseminate actionable intelligence, and report accurately on enemy intentions and capabilities.

The J-CD cell would be responsible for the installation, operation, and maintenance of the JFCCC computer network in place of a traditional J-6. Additionally, this cell would be assigned the information assurance (IA) mission. Since the JFCCC would focus on conducting operations in and through cyberspace, it would also possess offensive cyber capabilities. Consequently, the J-CA cell would be assigned responsibility for the computer network attack mission in place of a traditional J-3. Similar to the J-CE cell, the J-CD and J-CA cells would also have LNOs and representatives from appropriate national strategic and theater level agencies. Within the J-CD, NSA and DISA LNOs, along with onsite representation from the appropriate Regional Satellite Coordination Center (RSCC) and Standard Tactical Entry Points (STEP), should be considered. Likewise, the J-CA would have NSA and CIA LNOs. Finally, several civilian contractors and technical representatives from applicable software and hardware manufacturers would reside in the J-CA and J-CD in order to provide necessary subject matter expertise (e.g. Microsoft, Cisco, and Oracle) on different aspects of CNO.

Finally, a key JFCCC concern would be interagency coordination. Factor space-time is critical in cyberspace with the near instantaneous transmission speeds of modern C4 equipment. Therefore, close coordination between the JFCCC and national level agencies will always be necessary.[19] Although it would be abnormal for a FCC to bypass the GCC to coordinate and synchronize operations with other governmental agencies, the JFCCC will require direct liaison authority with NSA, the Central Intelligence Agency (CIA), and the Defense Information Systems Agency (DISA) during planning and operations. Streamlining the coordination process will allow the JFCCC to take advantage of the fleeting opportunities inherent in cyber operations.

The nature of cyberspace demands a fresh approach. In order to synchronize full spectrum cyber operations effectively within a JTF, a JFCCC must be established as a FCC. While this proposed JFCCC command and control structure is unique in many ways, it is befitting a complex JTF cyber mission. Future JTF Commanders can no longer afford to approach cyber defense, attack, and exploitation disparately. Ultimately, the JFCCC command and control structure is the best way to reduce the commander's span of control, improve unity of effort and command, and simplify cyber operations within a JTF.

[19] Offensive cyber operations will require close coordination with national strategic assets and capabilities at the National Security Agency (NSA). Likewise, defensive cyber operations involving the global information grid (GIG) will require close coordination with national strategic assets at the Defense Information Systems Agency (DISA).

Bibliography

United States House of Representatives, hearing before the Armed Services Committee on U.S. Cyber Command: Organizing for Cyberspace Operations, *"Statement of General Keith B. Alexander, Commander, United States Cyber Command,"* 23 September 2010. http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62398/pdf/CHRG-111hhrg62398.pdf (Accessed 12 December 2011)

United States House of Representatives, hearing before the Armed Services Committee on U.S. Strategic Command, "*Statement of General James E. Cartwright, Commander, United States Strategic Command,"* 21 March 2007. http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg37320/pdf/CHRG-110hhrg37320.pdf (Accessed 16 January 2012)

Congressional Research Service, report by John Rollins and Anna C. Henning entitled *"Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*," 10 March 2009.

_____, report by Clay Wilson entitled "*Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*," 20 March 2007.

Crowell, Richard M. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare v 1.5." Newport, R.I.: Naval War College.

Franklin, David M. "U.S. Command Relationships in the Conduct of Cyber Warfare: Establishment, Exercise, and Institution of Cyber Coordinating Authority." Newport, RI: Naval War College, 3 May 2010.

Gorman, Siobhan and Julian E. Barnes. "Cyber Combat: Act of War." *The Wall Street Journal*, 31 May 2011.

Hathaway, David C. "The Digital Kasserine Pass: The Battle Over Command and Control of DoD's Cyber Forces." *Foreign Policy at Brookings*, 15 July 2011.

Lewis, James A. "Multilateral Agreements to Constrain Cyberconflict." *Arms Control Today*, June 2010.

Libicki, Martin C. "Cyberdeterrence and cyberwar." Rand Corporation: Project Air Force, 2009.

Nakashima, Ellen. "Pentagon's Cyber Command seeks authority to expand its battlefield," *The Washington Post*, 6 November 2010.

Schaap, Arie J. "Cyber Warfare Operations: Development and Use Under International Law." *The Air Force Law Review*, 2009.

The Office of the President of the United States of America. *The Comprehensive National Cybersecurity Initiative.* Washington, D.C.: White House, March 2010.

_____. *The National Strategy to Secure Cyberspace*. Washington, D.C.: White House, 2003.

U.S. Department of Defense. Directive O-8530.1, *Computer Network Defense.* Washington, D.C.: Office of the Secretary of Defense, 9 January 2001.

_____. *Department of Defense Strategy for Operating in Cyberspace.* Washington, D.C.: DOD, July 2011.

_____. *Fiscal Year 2011-2015 Capability Gap Assessment Results and Recommendations for Mitigating Capability Gaps, JROCM 113-09*. Washington D.C.: DOD, June 2009.

_____. *Quadrennial Defense Review Report*. Washington D.C.: Office of the Secretary of Defense, February 2010.

_____. *Quadrennial Roles and Missions Review Report.* Washington D.C.: Office of the Secretary of Defense, January 2009.

_____. *Unified Command Plan*. Washington D.C.: Office of the Secretary of Defense, October 2008.

U.S. Government Accountability Office. *Report to Congressional Requesters, Defense Department Cyber Efforts – DOD Faces Challenges In Its Cyber Activities, GAO 11-75.* Washington, D.C.: GAO, July 2011.

_____. *Report to Congressional Requesters, Defense Department Cyber Efforts – More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities, GAO 11-421*. Washington, D.C.: GAO, May 2011.

U.S. Marine Corps. *Warfighting*, Marine Corps Doctrinal Publication (MCDP) 1. Washington, D.C.: Headquarters U.S. Marine Corps, 1986.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02. Washington, D.C.: CJCS, 12 April 2001 as amended through 31 July 2010.

_____. *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1. Washington, D.C.: CJCS, 2 May 2007 Incorporating Change 1, 20 March 2009.

_____. *Information Operations*, Joint Publication (JP) 3-13. Washington, D.C.: CJCS, 13 February 2006.

_____. *Joint Operations*, Joint Publication (JP) 3-0. Washington, D.C.: CJCS, 17 September 2006 Incorporating Change 2, 22 March 2010.

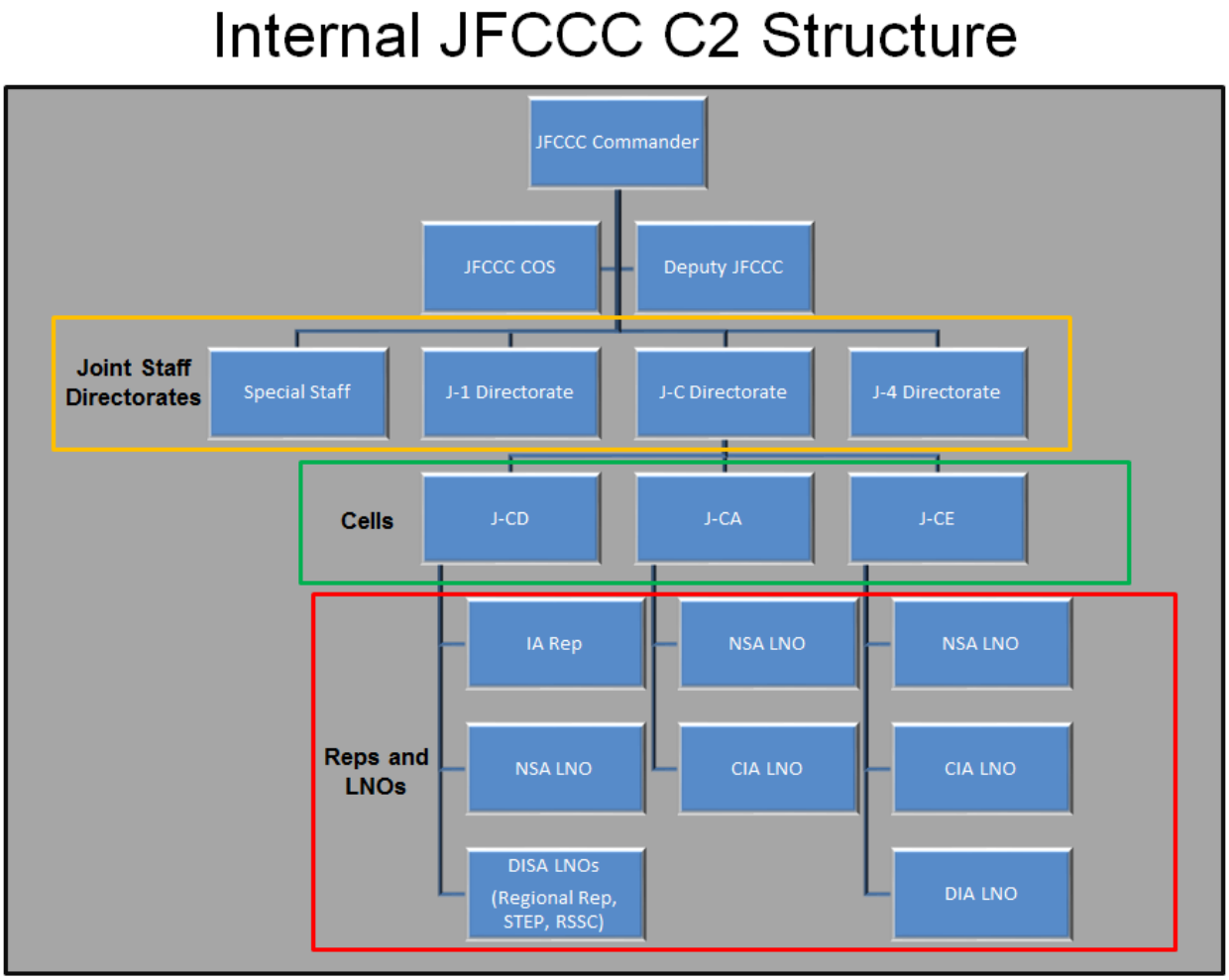
_____. *Joint Task Force Headquarters*, Joint Publication (JP) 3-33. Washington, D.C.: CJCS, 16 February 2007.

_____. *Management and Review of Joint Strategic Capabilities Plan (JSCP) – Tasked Plans.* Instruction 3141.01E, Washington, D.C.: CJCS, 15 September 2011.

_____. *Standing Rules of Engagement/Standing Rules for the Use of Force for U.S. Forces.* Instruction 3121.01B,Washington, D.C.: CJCS, 18 June 2008.

_____. *The National Military Strategy for Cyberspace Operations*. Washington D.C.: CJCS, December 2006.

Appendix A


Internal JFCCC C2 Structure
JFCCC Commander
JFCCC COS
Deputy JFCCC
Joint Staff Directorates
Special Staff
J-1 Directorate
J-C Directorate
J-4 Directorate
Cells
J-CD
J-CA
J-CE
Reps and LNOs
IA Rep
NSA LNO
NSA LNO
NSA LNO
CIA LNO
CIA LNO
DISA LNOs (Regional Rep, STEP, RSSC)
DIA LNO